

1

Review Midterm 1

Here are some informations about what you should know for the test...Feel free to ask me any questions about that during the week (even outside the regular office hours)!

1 Basic arithmetic

- Notion of divisibility, prime numbers, G.C.D.
- Euclidian division in \mathbb{Z} , the Euclidian algorithm (for the determination of a G.C.D.)
- Proof of: "The additive subgroups of \mathbb{Z} are the $n\mathbb{Z}$ "
- Definition of G.C.D(m,n) as the positive integer d such that $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$.
- Proof of : " $\sqrt{2} \notin \mathbb{Q}$."
- Definition of $\phi(n)$, $\phi(m.n) = \phi(m).\phi(n)$ if $G.C.D.(m, n) = 1$.

2 Congruences

- The ideals of the ring \mathbb{Z} are the $n\mathbb{Z}$
- definition of the ring $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ and how to compute with congruences.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ is an additive cyclic group.
- $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a field if and only if p is prime (you need to know how to prove this).
- The multiplicative group $(\mathbb{Z}/p\mathbb{Z}^\times, \times)$ is cyclic of order $p - 1$, when p is prime.
- Little Fermat's theorem.

3 Rings and ideals

- Definition of a ring, of a ring morphism, kernel and image of a ring morphism
- Definitions: of an ideal, sum of two ideals $(I + J)$, intersection, product of two ideals
- Quotient of a ring by an ideal

Theorem 1. (*Chinese Remainder Theorem*) Let I, J be two ideals of the ring R , such that $I + J = R$, then there is an isomorphism

$$R/(I.J) \simeq R/I \times R/J$$

given by

$$r \bmod I.J \longmapsto (r \bmod I, r \bmod J)$$

- Definition of the characteristic of a field
- In a field of characteristic p , one has $(x + y)^p = x^p + y^p$.

- If $f: R \rightarrow S$ is a ring morphism, then $f: R \rightarrow \text{im } f$ is surjective, and $\bar{f}: R/\ker f \rightarrow \text{im } f$ defined by $r \bmod \ker f \mapsto f(r)$ is well defined and is an isomorphism.
- $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$ as an example of the theorem just above.

4 Quadratic reciprocity

Definition 2. The **Legendre symbol** $\left(\frac{a}{p}\right)$, where p is an odd prime, and a is any integer is equal to $+1$ if a has a square root in $\mathbb{Z}/p\mathbb{Z}$, and -1 otherwise.

I would like you to know the following result and to have a vague idea of the proof

Theorem 3. (Legendre, Gauss) If p and q are two odd primes, then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

- $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$ and how to prove it.

5 Basic cryptography

- just know the R.S.A system (as it is explained at the beginning of the HW5).
- understand why there are 4 square roots of 1 in $\mathbb{Z}/p \cdot q\mathbb{Z}$, when p, q are two distinct primes (answer: chinese remainder theorem).